(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平10－116029

(43)公開日　平成10年(1998)５月６日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０９Ｃ　1/00	６１０	Ｇ０９Ｃ　1/00	６１０Ａ ６１０Ｂ

審査請求　未請求　請求項の数４　ＯＬ　（全７頁）

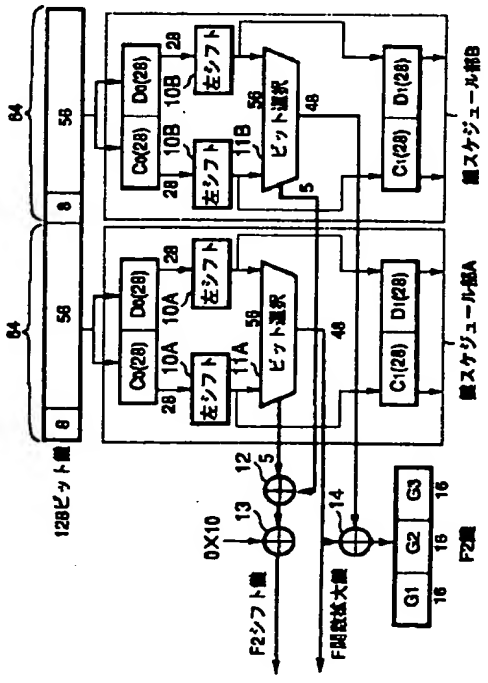
(21)出願番号　特願平8－269897

(22)出願日　平成８年(1996)10月11日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　佐野　文彦
福岡県福岡市東区筥松３－７－25　木栄荘201号
(72)発明者　櫻井　幸一
福岡県福岡市城南区七隈２－16－22
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　暗号化装置及び暗号化方法

(57)【要約】
【課題】ＤＥＳとの互換性を維持しつつ安全性を増大することができる暗号化装置を提供する。
【解決手段】所定のビット列からなる鍵情報を等分して得られる２つの暗号化鍵を、入力電文を攪拌するのに用いられる中間鍵にそれぞれ展開する同一構成の２つの鍵スケジュール部Ａ、Ｂと、この２つの鍵スケジュール部Ａ、Ｂから出力された２つの中間鍵に対して排他的倫理和を求める排他的倫理和１４と、この排他的論理和が０となることにより２つの中間鍵が互いに同一であることが検出された場合には、いずれか１つの中間鍵を用いて入力電文を攪拌するとともに、比較された２つの中間鍵が互いに同一でないことが検出された場合には、２つの中間鍵に基づいて入力電文を攪拌する攪拌部とを具備する。



1

【特許請求の範囲】

【請求項1】　入力電文を外部から入力された鍵情報に依存して攪拌し、対応する符号化電文を出力するデータ攪拌部と、

前記鍵情報を前記データ攪拌部に供給される中間鍵に展開する鍵スケジュール部とからなる暗号化装置であって、

前記鍵スケジュール部は、

鍵情報の半数のビットを一意の出力に対応づける鍵展開手段と、

外部から入力された前記鍵ビットの内、半数を前記鍵展開手段にて第1の中間鍵に展開すると共に、全鍵ビットの残りの半数に同じ処理を施して第1の中間鍵と同数のビットからなる第2の中間鍵に展開し、該第2の中間鍵と第1の中間鍵のビット毎に所定の演算を行なうことにより、第3の中間鍵を得る手段とを有し、

前記データ攪拌部は、

前記第1乃至第3の中間鍵の一部または全部のビットの値によって規定される攪拌処理を実現する複数の攪拌手段を有し、

前記複数の攪拌手段の内、第3の中間鍵のみによって規定される攪拌手段は、第3の中間鍵のビットの内、前記攪拌手段で用いられているビットが特定の条件を満たした場合には、前記攪拌手段への入力ビット列と同一のビット列を出力するように構成されていることを特徴とする暗号化装置。

【請求項2】　所定のビット列からなる鍵情報を複数個に分割して得られる複数の暗号化鍵を、入力電文を攪拌するのに用いられる中間鍵にそれぞれ展開する同一構成の複数の鍵展開手段と、

この複数の鍵展開手段から出力された複数の中間鍵を互いに比較する比較手段と、

この比較手段によって比較された複数の中間鍵が同一であることが検出された場合には、複数の中間鍵のいずれか1つを用いて入力電文を攪拌するとともに、

比較された複数の中間鍵が同一でないことが検出された場合には、複数の中間鍵のすべてに基づいて入力電文を攪拌する攪拌手段と、

を具備することを特徴とする暗号化装置。

【請求項3】　外部から入力された鍵情報を鍵スケジュール部において中間鍵に展開し、データ攪拌部においてこの中間鍵に依存して入力電文を攪拌して対応する符号化電文を出力する暗号化方法であって、

所定の鍵展開手段によって、外部から入力された鍵情報の内、半数のビットを第1の中間鍵に展開すると共に、前記鍵情報の残りのビットに同じ処理を施して第1の中間鍵と同数のビットからなる第2の中間鍵に展開し、

さらに、第1の中間鍵と第2の中間鍵との間でビット毎に所定の演算を行なうことにより、第3の中間鍵を得るとともに、

2

前記第1、第2、第3の中間鍵の一部または全部のビットの値によって規定される攪拌処理を行なうにあたって、第3の中間鍵のみによって規定される攪拌処理は、第3の中間鍵が特定の条件を満たした場合には、入力ビット列と同一のビット列を出力することを特徴とする暗号化方法。

【請求項4】　同一構成の複数の鍵展開手段によって、所定のビット列からなる鍵情報を複数個に分割して得られる複数の暗号化鍵を入力電文を攪拌するのに用いられる中間鍵にそれぞれ展開する展開工程と、

前記複数の鍵展開手段から出力された複数の中間鍵を互いに比較する比較工程と、

この比較工程において比較された複数の中間鍵が同一であることが検出された場合には、複数の中間鍵のいずれか1つを用いて入力電文を攪拌するとともに、

比較された複数の中間鍵が同一でないことが検出された場合には、複数の中間鍵のすべてに基づいて入力電文を攪拌する攪拌工程と、

を具備することを特徴とする暗号化方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は暗号化装置及び暗号化方法に関し、特に、秘密鍵ブロック暗号を用いた暗号化装置及び暗号化方法に関する。

【0002】

【従来の技術】ＤＥＳ (Data Encryption Standard) は、現在、最も広範に用いられている秘密鍵ブロック暗号系であり、文献、"Data Encryption Standard,"Federal Information Processing Standards Publication 46,National Bureau of Standards,U.S.Department of Commerce,1977. に詳細に記載されている。

【0003】ＤＥＳは６４ビット入力、６４ビット出力のブロック暗号であり、そのうち８ビットは鍵パリティ用として使用されるので５６ビットのみが実質的な鍵である。したがって、ＤＥＳが開発された当初からその安全性について議論がなされており、１９７７年に発表されて以来、さまざまな観点からの評価が行われている。その結果、１９９０年ごろに差分解読法や線形解読法といった鍵の全数探索よりも効率的な解読法が次々と提案された。特に、線形解読法を用いることにより、標準である１６段ＤＥＳの解読に成功している。

【0004】なお、差分解読法については、文献、E.Biham and A.Shamir,"Differential Cryptanalysis of DES-like Cryptosystems," Journal of CRYPTOLOGY,Vol.4,Number 1,1991に、線形解読法については、文献、松井充、“ＤＥＳ暗号の線形解読（Ｉ）”、暗号と情報セキュリティシンポジウム、ＳＣＩＳ９３－３Ｃ、１９９３に記載されている。

【0005】ＤＥＳが開発されてからの技術の発展や上記したような解読法を考慮すると、ＤＥＳには以下のよ

うな問題点があると考えられる。

（１）　現在のハードウェア技術の進歩を考えると処理を高速に行なうために１２８ビットのブロック暗号を構成することが可能であるが、いぜんとして６４ビットのブロック暗号を用いている。

（２）　Ｆ関数の構造に問題がある。ＤＥＳが開発された当時では、線形解読法が発案されておらず、線形解読法に対する耐性が考慮されていない。また、ハードウェア技術の発達の制約からＦ関数に含まれるＳ箱のテーブルサイズが小さい。現在のハードウェア技術のレベルを考えるとＳ箱のサイズをより大きくして安全性を高めることが望ましい。

（３）　５６ビットからなる鍵を用いているが、５６ビットの鍵の長さでは安全ではない。ハードウェアの発達により、現在では2^{56}個の鍵の組合せを調べるハードウェアの実現が可能である。また、専用のハードウェアを用いることにより、鍵の全数探索が可能であるとの発表もなされている。また、ＤＥＳの解読方法の１つである線形解読法は、鍵の一部のビットを解読により特定して残りのビットに対して全数検索を行なうものであるから、鍵を増やすことにより残りの鍵ビットの全数検索を行なう手間が増大して安全性が向上すると考えられる。

【０００６】上記した問題において、（３）のＤＥＳの鍵の長さに関する問題については、ＤＥＳチップをそのまま使用しながら鍵を長くする方法が考えられている。例えば、論文、B.Schneier,"Applied Cryptography," 2nd edition, Wiley (1996)は、ＤＥＳＸやTripleＤＥＳなどの暗号化方法を開示している。

【０００７】ＤＥＳＸはＤＥＳの入力及び出力の各々と６４ビットの鍵との排他的論理和をとる方法であるが、鍵の全数探索に対しては理論的な安全性が証明されている（J.Kilian and P.Rogaway, "How to protect ＤＥＳ against exhaustive key search," Proc. CRYPTO'96, pp.252-267(1996)を参照）。また、TripleＤＥＳはＤＥＳを３重に処理するアルゴリズムを用いているので、鍵の全数探索だけでなく、差分解読法や線形解読法に対しても、ＤＥＳ以上の安全性が確保できる。

【０００８】

【発明が解決しようとする課題】しかしながら、上記したＤＥＳＸは差分解読法や線形解読法に対してはＤＥＳと同等の安全性しか達成されない。また、TripleＤＥＳは構成が３倍になるので、処理速度はＤＥＳの処理速度の１／３となる。

【０００９】一方、上記した（１）、（２）で述べた問題点はＤＥＳの構造自体に関しており、これらを改良することは容易でない。また、これらを改良すれば本体のＤＥＳとは異なった暗号化処理を行なうことになり、ＤＥＳとの互換性の問題が新たに発生してしまう。

【００１０】本発明の暗号化装置及び暗号化方法はこのような課題に着目してなされたものであり、その目的とするところは、ＤＥＳとの互換性を維持しつつ安全性を増大することができる暗号化装置及び暗号化方法を提供することにある。

【００１１】

【課題を解決するための手段】上記の目的を達成するために、第１の発明に係る暗号化装置は、入力電文を外部から入力された鍵情報に依存して攪拌し、対応する符号化電文を出力するデータ攪拌部と、前記鍵情報を前記データ攪拌部に供給される中間鍵に展開する鍵スケジュール部とからなる暗号化装置であって、前記鍵スケジュール部は、鍵情報の半数のビットを一意の出力に対応づける鍵展開手段と、外部から入力された前記鍵ビットの内、半数を前記鍵展開手段にて第１の中間鍵に展開すると共に、全鍵ビットの残りの半数に同じ処理を施して第１の中間鍵と同数のビットからなる第２の中間鍵に展開し、該第２の中間鍵と第１の中間鍵のビット毎に所定の演算を行なうことにより、第３の中間鍵を得る手段とを有し、前記データ攪拌部は、前記第１乃至第３の中間鍵の一部または全部のビットの値によって規定される攪拌処理を実現する複数の攪拌手段を有し、前記複数の攪拌手段の内、第３の中間鍵のみによって規定される攪拌手段は、第３の中間鍵のビットの内、前記攪拌手段で用いられているビットが特定の条件を満たした場合には、前記攪拌手段への入力ビット列と同一のビット列を出力するように構成されている。

【００１２】また、第２の発明に係る暗号化装置は、所定のビット列からなる鍵情報を複数個に分割して得られる複数の暗号化鍵を入力電文を攪拌するのに用いられる中間鍵にそれぞれ展開する同一構成の複数の鍵展開手段と、この複数の鍵展開手段から出力された複数の中間鍵を互いに比較する比較手段と、この比較手段によって比較された複数の中間鍵が同一であることが検出された場合には、複数の中間鍵のいずれか１つを用いて入力電文を攪拌するとともに、比較された複数の中間鍵が同一でないことが検出された場合には、複数の中間鍵のすべてに基づいて入力電文を攪拌する攪拌手段とを具備する。

【００１３】また、第３の発明に係る暗号化方法は、外部から入力された鍵情報を鍵スケジュール部において中間鍵に展開し、データ攪拌部においてこの中間鍵に依存して入力電文を攪拌して対応する符号化電文を出力する暗号化方法であって、所定の鍵展開手段によって、外部から入力された鍵情報の内、半数のビットを第１の中間鍵に展開すると共に、前記鍵情報の残りのビットに同じ処理を施して第１の中間鍵と同数のビットからなる第２の中間鍵に展開し、さらに、第１の中間鍵と第２の中間鍵との間でビット毎に所定の演算を行なうことにより、第３の中間鍵を得るとともに、前記第１、第２、第３の中間鍵の一部または全部のビットの値によって規定される攪拌処理を行なうにあたって、第３の中間鍵のみによって規定される攪拌処理は、第３の中間鍵が特定の条件

5

を満たした場合には、入力ビット列と同一のビット列を出力する。

【００１４】また、第４の発明に係る暗号化方法は、同一構成の複数の鍵展開手段によって、所定のビット列からなる鍵情報を複数個に分割して得られる複数の暗号化鍵を入力電文を撹拌するのに用いられる中間鍵にそれぞれ展開する展開工程と、前記複数の鍵展開手段から出力された複数の中間鍵を互いに比較する比較工程と、この比較工程において比較された複数の中間鍵が同一であることが検出された場合には、複数の中間鍵のいずれか１つを用いて入力電文を撹拌するとともに、比較された複数の中間鍵が同一でないことが検出された場合には、複数の中間鍵のすべてに基づいて入力電文を撹拌する撹拌工程とを具備する。

【００１５】

【発明の実施の形態】以下、図面を参照して本発明の一実施形態を詳細に説明する。図１は本実施形態に係る暗号化装置の構成を示す図であり、入力電文としての平文（６４ビット）を外部から入力された鍵情報ｋに依存して撹拌し、対応する符号化電文を出力する第１段～第１６段から構成されるデータ撹拌部と、鍵情報ｋを前記データ撹拌部に供給される中間鍵に展開する鍵スケジュール部４とからなる。

【００１６】図１において、平文（６４ビット）は初期転置ＩＰが施された後、２つに等分されて左側３２ビットL_0と右側３２ビットR_0が生成される。一方、鍵スケジュール４には１２８ビットの鍵情報ｋが入力される。鍵スケジュール部４は以下に述べる方法によってＦ関数拡大鍵とＦ２鍵及びＦ２シフト鍵を生成して、データ撹拌部のＦ関数２とＦ２関数３にそれぞれ入力する。ここでＦ関数２は通常のＤＥＳと同様の撹拌処理を行なうものであり、Ｆ２関数３は以下に述べるような撹拌処理を行なう。

【００１７】Ｆ関数２はＦ関数拡大鍵とＦ２関数３の出力とを受けて所定の撹拌処理を行ってその結果を排他的論理和１に入力する。排他的論理和１はL_0（３２ビット）とＦ関数２の出力との間の排他的論理和を出力するが、これによって次段の右側３２ビットR_1が得られる。また、Ｆ２関数３の出力は次段の左側３２ビットL_1となる。

【００１８】以上の撹拌処理が第１段で行われ、L_1（３２ビット）とR_1（３２ビット）とが第２段に送られて第１段と同様の処理が施される。このようにして第１６段までの撹拌処理が行われた後、最終転置IP^{-1}が施されて暗号文（６４ビット）が得られる。

【００１９】このように本実施形態では、ＤＥＳの各段で使用される鍵のビット数を増加させるために、通常のＤＥＳの構成に加えて、各段の入力側（図１に示す位置）にＦ２関数を組み込んでいる。

【００２０】図２は図１に示す鍵スケジュール部４の１

6

段分の構成を示しており、ＤＥＳと同一の構成の鍵スケジュール部Ａと鍵スケジュール部Ｂとからなる。したがって鍵スケジュール部４はこのような構成の鍵スケジュール部を１６段設けた構成を有する。鍵スケジュール部Ａ、Ｂとも同一の処理を行なうのでここでは鍵スケジュール部Ａについてのみ説明する。

【００２１】１２８ビットの鍵情報は半分ずつに分割され、縮約型転置ＰＣ－１を施された後、５６ビットの鍵として各々の鍵スケジュール部に入力される。鍵（５６ビット）を２つに等分して生成した２８ビットからなる２つの鍵の各々C_0（２８ビット）、D_0（２８ビット）について左シフト部１０Ａで左シフト処理を施した後、ビット選択部１１Ａに入力する。ビット選択部１１Ａは所定のビット選択処理により４８ビットからなる第１の中間鍵と、５ビットからなる鍵とを出力する。この５ビットの鍵としては、５６ビット鍵の例えば、左から９、１８、２２、２５、３５番目の５ビットが用いられる。同様にしてビット選択部１０Ｂからは４８ビットからなる第２の中間鍵と、５ビットからなる鍵とが出力される。

【００２２】そして、ビット選択部１１Ａからの４８ビットの鍵とビット選択部１１Ｂからの４８ビットの鍵との間で排他的倫理和１４をとり、その結果としての４８ビットの第３の中間鍵を３等分して１６ビットの鍵Ｇ１、Ｇ２、Ｇ３を得る。この鍵Ｇ１、Ｇ２、Ｇ３をＦ２鍵としてＦ２関数３に入力する。

【００２３】同様に、鍵スケジュール部Ａのビット選択部１１Ａからの５ビットの鍵と、鍵スケジュール部Ｂのビット選択部１１Ｂからの５ビットの鍵との間で排他的論理和１２を求め、その結果と０Ｘ１０（０Ｘは１６進を表す）との間で排他的論理和１３をとったものをＦ２シフト鍵としてＦ２関数３に入力する。

【００２４】さらに、本実施形態では、鍵スケジュール部Ａのビット選択部１１Ａからの４８ビットの鍵をＦ関数拡大鍵としてＦ関数２に入力する。また、各々の２８ビットの鍵C_0（２８ビット）、D_0（２８ビット）を左シフトすることによって得られたC_1（２８ビット）、D_1（２８ビット）は次の段の鍵スケジュール部の入力となる。

【００２５】このように本実施形態では、ＤＥＳとの互換性を維持するために、１２８ビットの鍵を６４ビットずつに分割し、それぞれに対してＤＥＳの鍵スケジュール部Ａ、Ｂを適用している。また、Ｆ関数に入力される拡大鍵としては鍵スケジュール部Ａからの４８ビットの鍵をそのまま用いている。また、Ｆ２関数に用いる鍵としては鍵スケジュール部Ａからの４８ビット鍵と鍵スケジュール部Ｂからの４８ビット鍵とのビットごとの排他的論理和を１６ビットごとのブロックに分割して、それぞれＧ１、Ｇ２、Ｇ３としている。また、５６ビット鍵の左から特定番目の５ビットを選択してＦ２関数のシフ

ト鍵として用いている。

【００２６】図３はＦ２関数３の構成を示す図である。ここでは図１に示すＲ$_0$（３２ビット）を２つに等分して２つの１６ビットのブロックを生成する。左側の１６ビットブロックは排他的論理和２０に入力される。また、右側の１６ビットブロックは論理積２１と排他的論理和２２に入力される。

【００２７】論理積２１は１６ビット鍵Ｇ１と右側の１６ビット鍵との論理積をとって排他的論理和２０に入力する。排他的倫理和２０は左側の１６ビットブロックと論理積２１からの鍵との間で排他的論理をとり、その結果を左巡回シフト部２３に入力する。

【００２８】一方、排他的論理和２２は１６ビット鍵Ｇ２と右側の１６ビットブロックとの間で排他的倫理和をとり、その結果を左巡回シフト部２３に入力する。左巡回シフト部２３は、排他的論理和２０の出力と排他的論理和２２の出力からなる３２ビットの鍵に対して、入力された５ビットのＦ２シフト鍵を２進表記とみなして、そのビット数分の左巡回シフトを行なう。

【００２９】左巡回シフトを行った後の３２ビットの中間データの左半分の１６ビットはＦ２関数３の右半分の出力となる。また、左巡回シフトを行った後の３２ビットの中間データの右半分の１６ビットは排他的倫理和２４に入力される。

【００３０】論理積２５は１６ビットの鍵Ｇ３と左巡回シフトを行った後の３２ビットの中間データの左半分の１６ビットとの論理積をとってその結果を排他的論理和２４に入力する。排他的論理和２４はこの論理積と左巡回シフトを行った後の３２ビットの中間データの右半分の１６ビットとの間の排他的論理和をとり、その結果をＦ２関数３の左半分として出力する。

【００３１】上記したように、本実施形態のＦ２関数では、３２ビットの入力を１６ビットずつに分割して、分割された鍵とのビットごとの論理和や論理積をとっている。また、巡回シフト部ではＦ２シフト鍵のビット数だけ３２ビットの鍵に対して巡回シフトを行っている。

【００３２】以上の説明からわかるように、本実施形態の暗号化装置の利点はＤＥＳと同一の鍵スケジュール構成を用いていることにある。６４ビットの鍵を複製して１２８ビットの鍵を生成することにより、ＤＥＳとの完全な互換性を維持することができる。なぜなら、２つの鍵スケジュール部Ａ、Ｂの６４ビットの入力が同じであるならば、各スケジュール部で生成される中間鍵も同一のものとなる。各スケジュール部で生成される中間鍵が同一ならば両者のビットごとの排他的論理和１４は０となるため、Ｆ２関数３で用いられるＧ１、Ｇ２、Ｇ３も０となる。また同様に、排他的論理和１２の出力も０となり、Ｆ２シフト鍵は０Ｘ１０となる。

【００３３】このとき、図３に示すＦ２関数３の排他的論理和２０、２２の一方の入力が０となるので、Ｆ２関数３に入力された２つの１６ビットの鍵はそのまま左巡回シフト部２３に入力される。さらに、左巡回シフト部２３では鍵スケジュール部Ａ、Ｂからの２つの５ビット鍵の間の排他的論理和１２と０Ｘ１０との排他的倫理和１３をＦ２シフト鍵とし、このようなＦ２シフト鍵に基づいて左巡回を行っているので、Ｇ３＝０、すなわち、排他的論理和２４の一方の入力が０のときは、Ｆ２関数３に入力されたビット列（３２ビット）と同じビット列が出力されることになる。

【００３４】このようにして、２つの鍵スケジュール部Ａ、Ｂの６４ビットの入力が同じであるならば、Ｆ２関数３の構造は無視されることになるので、１２８ビット鍵の半分の６４ビットを鍵として用いたＤＥＳと全く同じ処理となり、互換性が満足される。

【００３５】さらに、本実施形態ではＦ２関数を加えたことによりＤＥＳと比較して各段でのデータ処理が増加することになるが、Ｆ２関数で用いられる演算は左巡回シフト命令、論理和、論理積、排他的論理和であり、これらの演算は通常多くのハードウェアに実装されているので高速処理が可能である。このことより、処理効率はＤＥＳと比較してあまり低下することはない。

【００３６】また、本実施形態ではＦ２関数での鍵の加え方に工夫を行っている。鍵を加える場合、入力データと鍵との排他的論理和をとる方法があるが、この方法では線形解読法を適用したときに排他的倫理和で加えられた鍵は解読の過程で比較的容易に導出されてしまい、鍵のビット数を増やしても安全性を高める効果が少ない。これに対して、本実施形態では、論理和や論理積を用いて鍵を加えているので、線形解読法による鍵の直接の導出は行われず、鍵のビット数の増加により強度の安全性の向上が計れる。

【００３７】以下に、ＯＳとしてSolaris2.5、コンパイラとしてgcc-2.7.2 を用い、最適化オプションなしのシステム環境下で、本実施形態の暗号化用サンプルソースプログラムを実行した場合のスループットを本実施形態とＤＥＳについて計測した。ここでは、上記サンプルソースプログラムからＦ２関数に関する部分を取り除いたものをＤＥＳの構成としている。

【００３８】計測の結果、図４（ａ）に示すような結果が得られた。スループットの速度比では本実施形態はＤＥＳの９０．６％であり、ＤＥＳを３重に構成したTripleＤＥＳがＤＥＳの１／３（すなわち、３３．３％）の速度であることと比較して十分高速であることがわかる。

【００３９】次に、ＯＳとしてLinux 、ＣＰＵとしてPentium 120MHz、コンパイラとしてgcc-2.7.2.1 、最適化オプションとして-02 を用いたシステム環境下で同様のサンプルソースプログラムを実行した場合のスループットを本実施形態とＤＥＳについて計測した。この場合も上記サンプルソースプログラムからＦ２関数に関する部

9

分を取り除いたものをＤＥＳの構成としている。

【００４０】計測の結果、図４（ｂ）に示すような結果が得られた。図４（ｂ）によれば、スループットの速度比では本実施形態はＤＥＳの６５％であり、ＤＥＳを３重に構成したTripleＤＥＳがＤＥＳの１／３の速度であることと比較してまだ十分高速であることがわかる。

【００４１】

【発明の効果】本発明によれば、ＤＥＳとの互換性を維持しつつ安全性を増大することができる暗号化装置及び暗号化方法を提供できる。

【図面の簡単な説明】

【図１】本発明の一実施形態における暗号化装置の構成

10

＊を示す図である。

【図２】図１に示す鍵スケジュール部４の１段分の構成を示す図である。

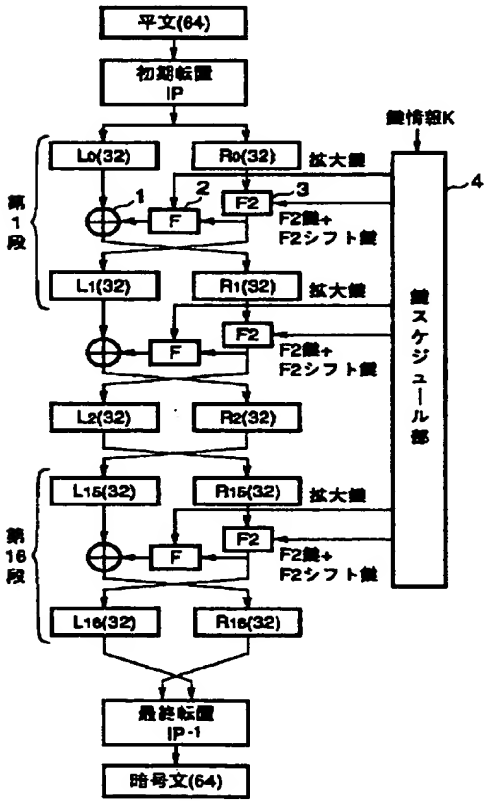
【図３】図１に示すＦ２関数の構成を示す図である。

【図４】本実施形態の暗号化方法に係るサンプルソースプログラムを実行した場合のスループットを本実施形態とＤＥＳについて計測した結果を示す図である。

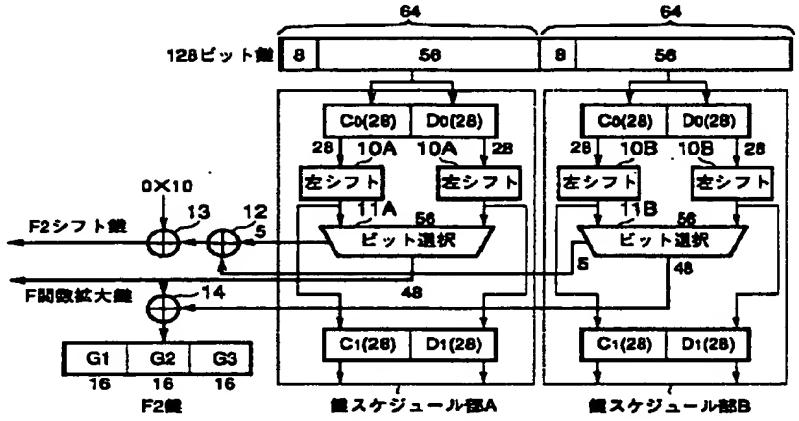
【符号の説明】

１…排他的論理和、２…Ｆ関数、３…Ｆ２関数、４…鍵スケジュール部、１０Ａ、１０Ｂ…左シフト部、１１Ａ、１１Ｂ…ビット選択部、１２、１３、１４…排他的論理和。

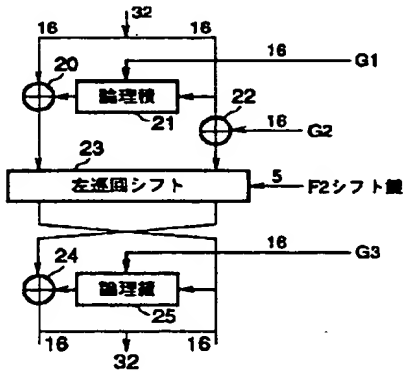
【図１】



【図２】



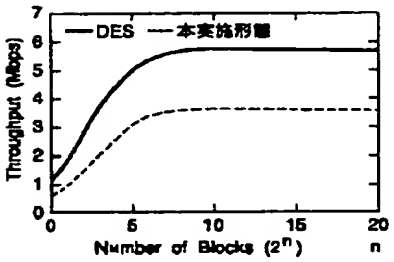
【図３】



【図４】

DES	本実施形態	速度比
64Kbps	58Kbps	90.6%

(a)



(b)